REMARKS

Claims 1-35, 69-79, 88, and 89 are pending. Claims 1, 69, 88, and 89 are in independent form.

Rejections under 35 U.S.C. § 102

Claim 1 was rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,477,651 to Teal et al. (hereinafter "Teal").

Claim 1 relates to a machine-implemented method for automatically identifying common content to use in identifying an intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, and analyzing a plurality of said reduced data items to detect common elements, said analyzing identifying common content indicative of a network attack. The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

Teal neither describes nor suggests several features of claim 1. For example, Teal neither describes nor suggests that a collection of data items that is to be analyzed to identify a network attack be reduced to a reduced data collection, as recited in claim 1. As another example, Teal neither describes nor suggests that a plurality of such reduced data items be analyzed to detect common elements, said analyzing reviewing for common content indicative of a network attack, as recited in claim 1.

The basis for these deficiencies in Teal arises from a fundamental difference between Teal's focus and the subject matter recited in claim 1. In particular, claim 1 relates to a "method for automatically identifying common content to use in identifying an intrusive network attack."

In contrast, Teal's primary focus is on loading signatures (i.e., specific patterns in network traffic, audit trails, and other data sources that indicate malicious activity) into an intrusion detection system. *See, e.g., Teal*, col. 1, line 56-63; col. 4, line 32-36. For example, Teal allows an intrusion detection system to remain running while new signatures are loaded. *See, e.g., Teal*, col. 3, line 23-27. As another example, Teal specifically directs individual analysis object towards detecting attacks on each network vulnerability. *See,*

e.g., *Teal*, col. 3, line 29-33. Teal accomplishes this by loading analysis objects as plug-ins that are tailored to the needs of a particular network. *See, e.g., id.*

With Teal primarily concerned with loading signatures into an intrusion detection system, it is perhaps not surprising that Teal does not provide many details as to how those signature are determined. Instead, Teal describes that network data is converted into predetermined formats for analysis and that this network data is analyzed to look for specific patterns that indicate malicious activity. *See, e.g., Teal*, col. 4, line 16-20; col. 4, line 28-33. Teal does not provide many details regarding how those specific patterns are identified.

Accordingly, claim 1 is not anticipated by Teal. Applicant respectfully requests that the rejections of claim 1 and the claims dependent therefrom be withdrawn.

Rejections under 35 U.S.C. § 103

Claim 69 was rejected under 35 U.S.C. § 103(a) as obvious over Teal and U.S. Patent No. 7,089,592 to Adjaoute (hereinafter "Adjaoute").

Claim 69 relates to a machine-implemented method for automatically identifying common content to use in identifying an intrusive network attack. The method includes monitoring network content on a network and obtaining at least portions of

the data on said network, data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion, analyzing said reduced data portions to find network content which repeats a specified number of times in order to establish said network content which repeats said specified number of times as frequent content, identifying address information of said frequent content, and identifying the frequent content as associated with the network attack based on said identifying and determining.

The address information includes at least one of source information or destination information that characterizes the respective of sources and/or destinations of said frequent content and determining if a number of sources and/or destinations of said frequent content is increasing.

The rejection of claim 69 simply states that claim 69 is "[r]ejected under the same rational as claim 1." *See Office action mailed August 11, 2008*, page 14, line 2.

Applicant respectfully disagrees with the rejection for several reasons. For example, Teal and Adjaoute neither describe nor suggest that portions of the data on a network are to be obtained and data reduced, as recited in claim 69. As

another example, Teal and Adjaoute neither describe nor suggest that such reduced data portions be analyzed to find network content which repeats a specified number of times in order to establish said network content as frequent content, as recited in claim 69.

The basis for these deficiencies in Teal arises from a fundamental difference between Teal's focus and the subject matter recited in claim 69. In particular, claim 69 relates to a "method for automatically identifying common content to use in identifying an intrusive network attack." As discussed above, Teal is primarily concerned with loading signatures into an intrusion detection system and does not provide many details as to how those signature are identified.

Adjaoute does nothing to remedy these deficiencies in Teal. In this regard, Adjaoute describes a single and common software solution that detects and prevents electronic fraud and network intrusion in real-time. *See, e.g., Adjaoute*, col. 7, line 64-col. 8, line 5. Adjaoute's software solution consists of three main components, namely, (1) a fraud detection and prevention model component, (2) a model training component, and (3) a model querying component. *See, e.g., Adjaoute*, col. 7, line 64-col. 8, line 5. *See, e.g., Adjaoute*, col. 8, line 12-17. Adjaoute's fraud detection and prevention model component takes data associated with a user's network activity and decides whether

the user is breaching network security. *See, e.g., Adjaoute*, col. 8, line 21-23. The model consists of an extensible collection of integrated sub-models, each of which contributes to the final decision. *See, e.g., Adjaoute*, col. 8, line 23-25. The model contains four default sub-models and four extension, namely, (1) a data mining sub-model, (2) a neural network sub-model, (3) a multi-agent sub-model, (4) a case-based reasoning sub-model, (5) a rule-based reasoning sub-model, (6) a fuzzy logic sub-model, (7) a sub-model based on genetic algorithms, and (8) a constraint programming sub-model. *See, e.g., Adjaoute*, col. 8, line 25-31; col. 14, line 35-47.

Adjaoute describes each of these sub-models in additional detail. *See, e.g., Adjaoute*, col. 14, line 48-64 (describing the neural network sub-model); col. 16, line 49-63 (describing the multi-agent sub-model); col. 18, line 44-57 (describing the data mining sub-model); col. 20, line 13-28 (describing case-based reasoning sub-model); col. 21, line 10-32 (describing genetic algorithm sub-models, rule-based reasoning sub-models, fuzzy logic sub-models, and constraint programming sub-models).

None of these various sub models obtain portions of the data on a network data reduces them, as recited in claim 69. Further, none of these various sub models analyzes such reduced

data portions to find network content which repeats a specified number of times in order to establish said network content as frequent content, as recited in claim 69.

If the examiner persists in maintaining the rejection, applicant respectfully requests that the particular sub-model which allegedly performs these and the other activities recited in claim 69 be identified with sufficient particularity to allow Applicant to judge the propriety of continuing prosecution. *See* 35 U.S.C. § 132 and 37 C.F.R. § 1.104(2).

In the absence of such a showing, even if Teal and Adjaoute were combined, one of ordinary skill would not arrive at the subject matter recited in claim 69. Accordingly, claim 69 is not obvious over Teal and Adjaoute. Applicant respectfully requests that the rejections of claim 69 and the claims dependent therefrom be withdrawn.

Claim 88 was rejected under 35 U.S.C. § 103(a) as obvious over Teal and Adjaoute.

Claim 88 relates to a machine-implemented method for automatically identifying common content to use in identifying an intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to

determine frequently occurring sections of message information indicative of a network attack, and carrying out an additional test on said frequently occurring sections of message information.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

The rejection of claim 88 is understood to contend that it would have been obvious for one of ordinary skill to have combined Teal and Adjaoute to have arrived at the recited subject matter.

Applicant respectfully disagrees with the rejection for several reasons. For example, Teal and Adjaoute neither describe nor suggest that a collection of data items to be analyzed to identify the network attack is to be obtained and data reduced, as recited in claim 88. As another example, Teal and Adjaoute neither describe nor suggest that a plurality of such reduced data items be analyzed to determine frequently occurring sections of message information indicative of a network attack, as recited in claim 88.

As discussed above, Teal is primarily concerned with loading signatures into an intrusion detection system and does not provide many details as to how those signature are identified. As for Adjaoute, none of the various sub models performs these activities.

If the examiner persists in maintaining the rejection, applicant respectfully requests that the basis for the rejection be stated with sufficient particularity to allow Applicant to judge the propriety of continuing prosecution, as required by 35 U.S.C. § 132 and 37 C.F.R. § 1.104(2).

In the absence of such a showing, even if Teal and Adjaoute were combined, one of ordinary skill would not arrive at the subject matter recited in claim 88. Accordingly, claim 88 is not obvious over Teal and Adjaoute. Applicant respectfully requests that the rejection of claim 88 be withdrawn.

Claim 89 was rejected under 35 U.S.C. § 103(a) as obvious over Teal and Adjaoute.

Claim 89 relates to a machine-implemented method for automatically identifying common content to use in identifying an intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items comprise a first subset of a network packet including payload and header, reducing said data items in said collection to reduce said data collection to a

reduced data collection of reduced data items, analyzing a plurality of said reduced data items to detect common elements, and obtaining a second subset of the same network packet for subsequent analysis.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

The rejection of claim 89 is understood to contend that it would have been obvious for one of ordinary skill to have combined Teal and Adjaoute to have arrived at the recited subject matter.

Applicant respectfully disagrees with the rejection for several reasons. For example, Teal and Adjaoute neither describe nor suggest that a collection of data items to be analyzed to identify the network attack is to be obtained and reduced, as recited in claim 89. As another example, Teal and Adjaoute neither describe nor suggest that a plurality of such reduced data items be analyzed to detect common elements, as recited in claim 89.

As discussed above, Teal is primarily concerned with loading signatures into an intrusion detection system and does not provide many details as to how those signature are identified. As for Adjaoute, none of the various sub models performs these activities.

If the examiner persists in maintaining the rejection, applicant respectfully requests that the basis for the rejection be stated with sufficient particularity to allow Applicant to judge the propriety of continuing prosecution, as required by 35 U.S.C. § 132 and 37 C.F.R. § 1.104(2).

In the absence of such a showing, even if Teal and Adjaoute were combined, one of ordinary skill would not arrive at the subject matter recited in claim 89. Accordingly, claim 89 is not obvious over Teal and Adjaoute. Applicant respectfully requests that the rejection of claim 89 be withdrawn.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to

concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: November 10, 2008

/John F. Conroy, Reg. #45,385/
John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

JFC/jhg
14003896.doc